§170.315(d)(12) Encrypt authentication credentials

2015 Edition CCGs

Version 1.0 Updated on 06-15-2020

Revision History

Version #	Description of Change	Version Date
1.0	Initial Publication	06-15-2020

Regulation Text

Regulation Text

§170.315 (d)(12) *Encrypt authentication credentials*. Health IT developers must make one of the following attestations and may provide the specified accompanying information, where applicable:

(i) Yes – the Health IT Module encrypts stored authentication credentials in accordance with standards adopted in § 170.210(a)(2).

(ii) No – the Health IT Module does not encrypt stored authentication credentials. When attesting "no," the health IT developer may explain why the Health IT Module does not support encrypting stored authentication credentials.

Standard(s) Referenced

Paragraph (d)(12)(i)

§ 170.210(a)(2) *General*. Any encryption algorithm identified by the National Institute of Standards and Technology (NIST) as an approved security function in Annex A of the Federal Information Processing Standards (FIPS) Publication 140-2, October 8, 2014 (incorporated by reference in §170.299).

Certification Companion Guide: Encrypt authentication credentials

This Certification Companion Guide (CCG) is an informative document designed to assist with health IT product development. The CCG is not a substitute for the 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program Final Rule (ONC Cures Act Final Rule). It extracts key portions of the rule's preamble and includes subsequent clarifying interpretations. To access the full context of regulatory intent please consult the ONC Cures Act Final Rule or other included regulatory reference. The CCG is for public use and should not be sold or redistributed.

Link to Final Rule Preamble

Edition Comparision	Gap Certification Eligible	Base EHR Definition	In Scope for CEHRT Definition
New	No	Not Included	No

Technical Explanations and Clarifications

Applies to Entire Criterion

Clarifications:

- The criterion does not require certified health IT to have these capabilities or for health IT developers to implement these capabilities for a specific use case or any use case, just that they attest “yes” or “no” to whether the Health IT Module encrypts authentication credentials. The criterion places no requirements on health IT customers, such as health care providers, to implement these capabilities (if present in their products) in their health care settings.

Paragraph (ii)

Clarifications:

- If a health IT developer attests “no” for its Health IT Module(s) it can indicate why the Health IT Module(s) does not support encrypting stored authentication credentials. For example, the health IT developer could explain that its Health IT Module is not designed to store authentication credentials; therefore there is no need for the Health IT Module to encrypt authentication credentials.

Content last reviewed on June 17, 2020